# QoS Recovery Schemes Based on Differentiated MPLS Services in All-Optical Transport Next Generation Internet

Jigesh K. Patel, Sung U. Kim, and David H. Su
National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899, USA
{patel, kimsu, dsu}@antd.nist.gov

## Abstract

The Internet is evolving from best-effort service toward an integrated or differentiated service framework with Quality-of-Service (QoS) assurances that are required for new multimedia service applications. Given this increasing demand for high bandwidth Internet with QoS assurances in the coming years, an IP/MPLS-based control plane combined with a wavelength-routed Dense Wavelength Division Multiplexing (DWDM) optical network is seen as a very promising approach for the realization of future re-configurable transport networks. Fault and attack survivability issues concerning physical security in a DWDM All-Optical Transport Network (AOTN) require a new approach taking into consideration AOTN physical characteristics. Furthermore, unlike in electronic networks that regenerate signals at every node, attack detection and isolation schemes may not have access to the overhead bits used to transport supervisory information between regenerators or switching sites to perform their functions. This paper presents an analysis of attack and protection problems in an AOTN. Considering this, we propose a framework for QoS guarantees based on the Differentiated MPLS Service (DMS) model and QoS recovery schemes against QoS degradation caused by devices failures or attack-induced faults in an AOTN. We also suggest how to integrate our attack management model into the NIST's simulator – Modeling, Evaluation and Research of Lightwave Networks (MERLiN).

## Keywords

WDM, IP/MPLS, intrusion management, quality-of-service, all-optical transport networks, next generation Internet.

***CONTACT AUTHOR***

**Jigesh K. Patel (jigesh_patel@yahoo.com)**
**RSoft, Inc.,**
**200 Executive Boulevard,**
**Ossining, NY 10562, USA**

**Fax: 1-914-736-9823**

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **JAN 2002** | | **00-00-2002 to 00-00-2002** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **QoS Recovery Schemes Based on Differentiated MPLS Services in All-Optical Transport Next Generation Internet** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Institute of Standards and Technology,Gaithersburg,MD,20899** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES
**Photonic Network Communications, Vol 4, No. 1, pp. 5-18, Jan. 2002**

14. ABSTRACT
**see report**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **20** | |

## 1. Introduction

Recent advances in the IP-MPL(λ)S -based control plane are being combined with optical cross connect (OXC) technology to provide recovery with Quality of Service (QoS) guarantee. However, QoS degradation caused by device failures or attack-induced faults in AOTN requires service-specific QoS recovery methods with emphasis on an appropriate recovery path.

In today's best effort Internet, variable queuing delays on network routers, intermittent latency, and dropped packets from congested links make it difficult to provide an acceptable level of performance. The Integrated Services (IntServ) architecture [1] was first introduced along with the Resource ReSerVation Protocol (RSVP) [2]. The Differentiated Services (DiffServ) architecture [3], as a more scalable solution, classifies packets into a small number of aggregated flows or service classes specifying a particular forwarding treatment or per hop behavior (PHB). Even if DiffServ defines a model for implementing scalable differentiation of QoS in the Internet, it cannot give any solution to a problem of asymmetric traffic distribution for premium service [4]. DiffServ alone cannot solve this problem caused by the absence of a traffic control mechanism. However, within the Multi-Protocol Label Switching (MPLS) architecture, the DiffServ mechanism and traffic engineering associated with constraint-based routing could avoid this congestion.

Tremendous potential for capacity expansion offered by Wavelength Division Multiplexing (WDM) is revolutionizing the way we look at an AOTN. Our experience with the present form of Internet has compelled us to provision for enough recovery measures against any kind of hacking possibilities. However, unlike in the case of legacy Time Division Multiplexing (TDM) traffic, the WDM traffic demands additional intrusion management concerns. These include attention at the physical device level.

This paper presents an analysis of attack and recovery problems in the AOTN. Based on this analysis, we propose a framework for QoS guarantee based on the DMS model and the QoS recovery aspect for QoS degradation caused by device failures or attack-induced faults in the AOTN. Our differentiated QoS protection/restoration schemes take into account the service quality sensitive aspects, like type of layer protection/restoration to be invoked, recovery speed, and resource reservation style, in order to locate an idle link or path capable of sustaining the necessary QoS. In Section 2, we analyze the architecture of the AOTN and network survivability as well as QoS recovery concepts. Section 3 discusses the DMS architecture with QoS Recovery. Section 4 explains QoS recovery against QoS degradation caused by attack-induced faults. Conclusion and how to integrate our attack survivability management functions to MERLiN are presented in Section 5.

## 2. All-Optical Transport Network and Network Survivability

### 2-1. All-Optical Transport Network for Next Generation Internet [5]

Core transport networks are currently in a period of transition, evolving from SONET/SDH-based TDM networks with WDM used strictly for fiber capacity expansion, toward WDM-based all optical networks with transport, multiplexing, routing, supervision, and survivability at the optical layer. Moreover, given that the IP protocol framework will become a dominant form of data transfer in the

future, there has been an increasing interest in the implementation of IP over photonic networks by using optical networking. A consensus is emerging in the industry on utilizing an IP-centric control plane within optical networks to support dynamic provisioning and restoration of lightpaths. Specifically, we note that IP routing protocols and MPLS or Multi-Protocol Lambda Switching (MPλS) signaling protocols could be adapted for optical networking needs.

Within the AOTN framework for implementing the Next Generation Internet (NGI), a key issue is how to combine the advantages of the relatively coarse-grained WDM techniques with optical switching capabilities to yield a high-throughput optical platform able to efficiently control the IP traffic. The main issue while designing optical networks for Internet application is specifying the right transport/control modalities for IP packets. Actually, several transport/control options have been proposed by several standards organizations and industry consortia, such as IP over ATM over WDM, and IP over SDH/SONET over WDM; and the recent trend favors IP over WDM. The IP/MPLS (or MPλS) based control plane combined with DWDM technology, makes it possible to provide a framework for optical bandwidth management and real time provisioning of optical channels in an automatically switched, transparent optical network. Actually, in the the IETF, generalized-MPLS (G-MPLS) signaling is defining extensions to MPLS routing and signaling protocols for application to optical networks. Figure 1 illustrates a currently agreed upon layered framework for IP/MPLS over WDM via the optical adaptation layer.

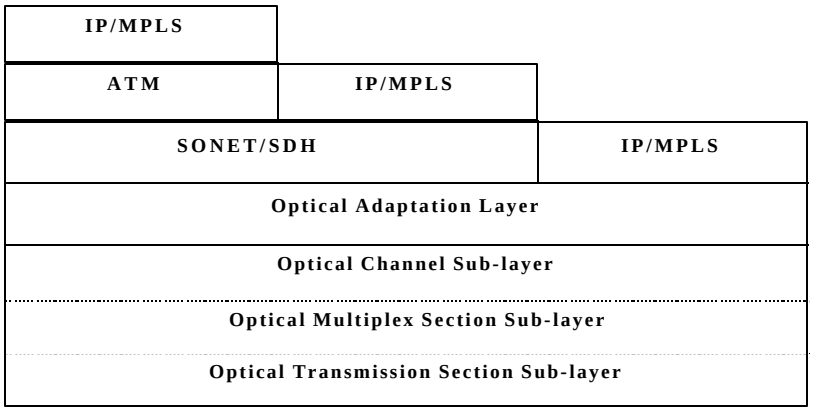



Figure 1. IP/MPLS over WDM

Global standards for the Optical Transport Network (OTN) are under development at the ITU-T. The layered architecture of optical networks is standardized in ITU-T G.872, whereby in an equivalent layered network modeling as defined in the ITU-T standards for Optical Transport Networks (OTN), a WDM node can be represented by the following hierarchical layers (from top to bottom): Optical Channel layer (OCh), Optical Multiplex Layer (OMS) and the Optical Transmission Layer (OTS). The OTS layer provides optical signal propagation functionality and represents transmission medium, taps, and amplification modules. The OMS layer enables wavelength routing that provides functionality for networking of a multi-wavelength optical signal and the OCh layer handles the channel for information

content of varying formats. In the Optical Internetworking Forum (OIF) and ANSI T1X1.5, the proposals for implementing frame-monitoring layer overhead information as a function of the optical adaptation layer, include the use of a TDM frame-like "SONET-lite" or "digital wrapper" to support OCh (Optical Channel) layer management functions such as performance monitoring, connectivity, and fault indicator monitoring. On the other hand, the Automatic Switched Optical Network (ASON) is a framework that specifies the requirements and architecture of the control and management of an automatic switched optical transport network. Accepted as a study item by SG13 of the ITU-T in March 2000, G.ASON describes several signaling interfaces whose combination can enable a service capability with end-to-end dynamic connectivity in the optical transport network.

AOTN is a network where the user-network interface is optical and data does not undergo optical to electronic conversion within the transport network. An architectural model for AOTN is depicted in Figure 2.

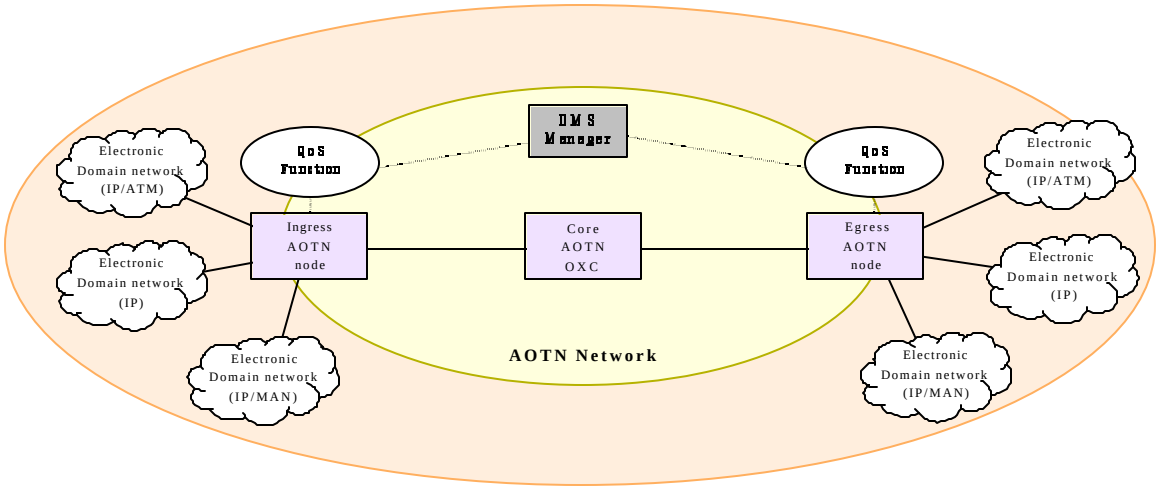



Figure 2. An architectural model of AOTN

The optical components that constitute a WDM node, in general, include a cross-connect switch (with or without wavelength conversion functionality) consisting of opto-mechanical switches, a demultiplexer comprising of signal splitters and optical filters, and a multiplexer made up of optical filters, and signal combiners. Optical Cross-Connects (OXCs) provide the routing capabilities for establishing lightpaths throughout the network.

As shown in Figure 2, there are two functional control domains. The external one is the electronic control domain, where the routing/forwarding functions based on packet header processing should be performed. On the other hand, the internal one is the optical control domain so as to access the huge fiber bandwidth that performs transmission and low-layer switching functions based on optical technology. IP traffic is injected into the ingress AOTN node by a variety of conventional electronic domain legacy networks (i.e., LANs, MANs, ATMs, etc.). The ingress node performs traffic aggregation and basic routing functions to a given destination egress node for a data packet. In order to simplify the packet

forwarding process within the optical nodes, the MPLS concept is used at the ingress and egress nodes. Note that MPλS has been proposed [6] within the IETF as an extension of MPLS for optical networks. In this scheme, Optical channels are viewed as analogous to labels in MPLS.

Once the data packet is organized, the AOTN transports the packets from source to destination nodes through a lightpath. A lightpath is an end-to-end path of wavelength that is established between an ingress and egress node pair. The wavelengths are capable of being dynamically switched inside the optical network by the OXCs that are not sensitive the signal itself, but only to the wavelength over which it is carried. Such routing is called wavelength routing and renders the lightpaths transparent to variables such as modulation format, bit-rate, and protocol type. A fiber segment carries high-speed data flows, consisting of many time-division multiplexed channels associated with optical channels. At the destination egress node, the traffic is de-segregated and delivered to the destination network. The core AOTN OXC switches are interconnected via a WDM optical transport network and perform forwarding of the data packets in the all-optical signal domain.

Over the past decade, the exponential growth of Internet traffic volumes has made the IP protocol framework becoming the most predominant networking technology. Furthermore, the Internet is evolving from best-effort service toward an integrated or differentiated service framework with QoS assurances which will be necessary for new applications such as voice telephony, video conferencing, tele-immersive virtual reality, and Internet games. Given this increasing demand for high bandwidth Internet with QoS assurances in the coming years, IP/MPLS (or MPλS) based a control plane combined with a wavelength-routed DWDM optical network is seen as a very promising approach for the realization of future re-configurable transport network.

### 2-2. Network Survivability and QoS Recovery

In general, network survivability and QoS recovery in AOTNs can be summarized as illustrated in Figure 3.

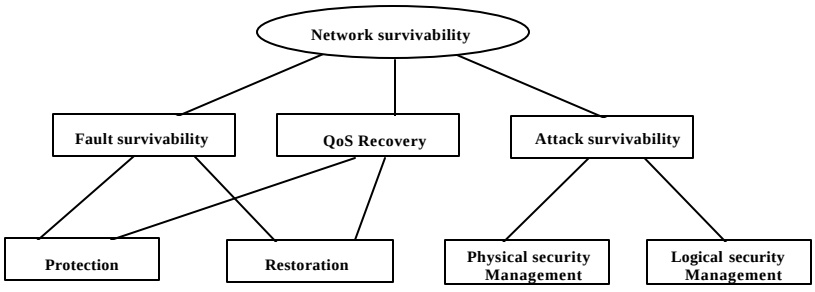



Figure 3. Network survivability and QoS recovery in AOTNs

The main goals of fault/attack survivability (fault/attack management) are to set up routes in anticipation of faults/attacks (protection), locate the faults/attacks (detection and localization), and to re-route the affected connections (restoration). Protection is the primary mechanism used to deal with faults/attacks. In protection, preplanned protection resources (fibers, nodes, etc.) are set aside for restoring

traffic when the working path is established. On the other hand, restoration dynamically discovers an alternate route from spare resources in the network for disrupted traffic, once a fault or attack is detected.

Although many researchers are actively working on fault supervisory management and protection/restoration schemes for AOTNs, many adaptations have been obtained from schemes previously investigated for electronic based networks. For attack detection and protection/restoration endeavors for AOTNs, some researchers have proposed attack detection and management schemes for amplifiers or fiber level partially [7]. However, attack detection and protection/restoration schemes for every attack possible at network elements are still in their infancy.

Fault/attack detection is one of the crucial functions and a prerequisite for the above mentioned protection/restoration schemes. The inability of AOTNs to reconstruct data streams at nodes within transparent networks complicates segment-by-segment monitoring of communication links. Nevertheless, many common faults (such as fiber cuts and node malfunctions) may be detected by optical monitoring methods. On the other hand, a resourceful attacker may thwart detection with the relatively simple monitoring methods available now. Although research on attack survivability for the AOTN is relatively scant, many interesting issues exist [7].

The management of attacks also involves the protection of data security. This security can be considered at the logical (or semantic) level to protect the information content of the data if an attacker is able to access them. Many of the traditional security problems related to logical security present in traditional electronic networks are still present in AOTNs. However, the approach for logical security (like, encryption, privacy, and authentication) taking into consideration AOTN physical characteristics opens up avenues for further research.

QoS restorability in optical networks is introduced in [8] as a performance measure for service-specific restoration methods applied to wavelength connections. However, the protection/restoration methods proposed so far (including those based on MPλS) do not take into account QoS degradation related to the physical device characteristics in the AOTN. Moreover QoS degradation led by device failures or attack-induced faults in the AOTN, requires service-specific recovery methods with emphasis on an appropriate recovery path so as to guarantee the necessary QoS. In this paper, we restrict our discussion to the QoS recovery aspect as applied to the degradation of QoS led by device failures or attack-induced faults.

## 3. Differentiate MPLS Services (DMS) Architecture with QoS Recovery

### 3-1. Traffic Classes in the Next Generation Internet

Generic classification of application types supported on the NGI may be divided into (a) applications that do require absolute guarantees on QoS, (b) those requiring certain minimal statistical guarantees on QoS, and (c) those that do not require explicit QoS guarantees. Class 1 (type a) encompasses all constant bit rate application flows characterized by deterministic packet rates and sizes. As inelastic real time traffic, it is also characterized by low tolerance to delays and delay variability; and relatively high tolerance to packet loss. Examples include provisioned connections such as virtual leased lines or switched services such as voice and video circuits.

Network traffic class 2 (b) has variable statistical attributes similar to class 3 (c) but demands certain minimal statistical guarantees on QoS, and exhibits a greater degree of time-sensitivity. Distributed simulation and real-time streaming are as examples under this class. Actually the end-to-end integrity of class 2 Variable Bit Rate (VBR) service may be assured by employing reliable stream protocols similar to TCP. Otherwise applications that subscribe to class 3 (c), such as best effort service or web browsing, are allowed to inject VBR traffic at any arbitrary rate into the network. This service tries to make the best use of the remaining bandwidth. The end-to-end reliability of class 3 data flows may be reinforced by TCP-like reliable stream protocols.

### 3-2. DMS Architecture and Service

A major consideration in designing a Differentiated MPLS Service (DMS) is the issue of scalability. This can be achieved by flow aggregation, thereby ensuring individual end-to-end QoS guarantees without maintaining knowledge base of individual flows on each segment of their paths. This implies that a heavy computational overhead can be avoided in core nodes by manipulating and maintaining the state of QoS for each aggregated traffic flow in the edge node. In the QoS functions of an ingress AOTN node as given in Figure 4 (see also the DMS domain as illustrated in Figure 2), functions such as classification, marking, and policing would be needed only at the edge level AOTN nodes of the network. The core AOTN nodes only implement forwarding of the data packets in the all-optical signal domain. While the edge AOTN nodes have the same capabilities as the core AOTN nodes, they use policing to monitor the customer contract and a classifier, and mark the traffic at the incoming interface. Another important consideration in designing a DMS is that for the MPLS network, a recovery priority could be used as a differentiating mechanism to support the service requiring higher reliability.

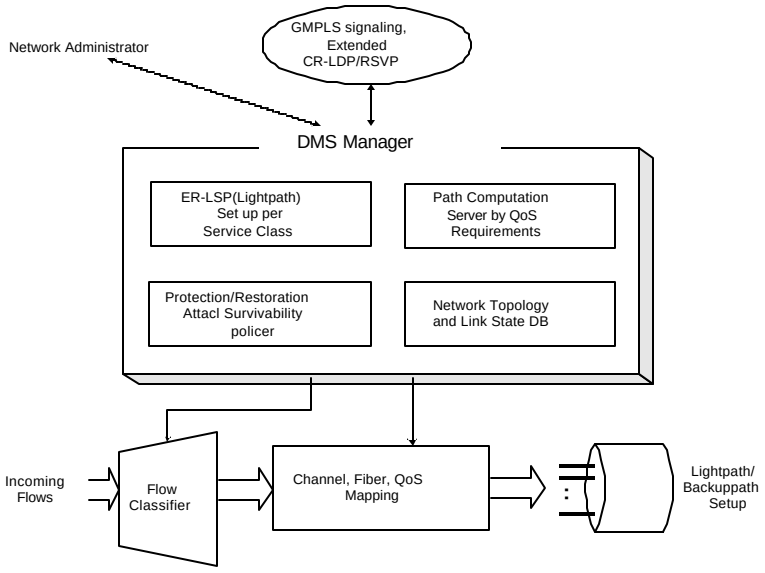
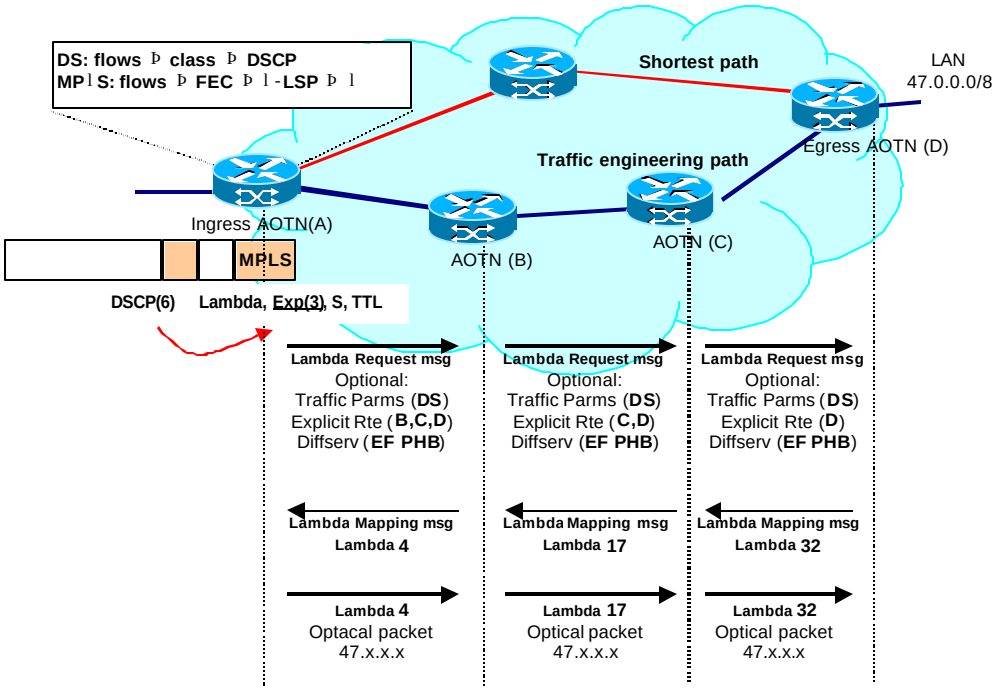


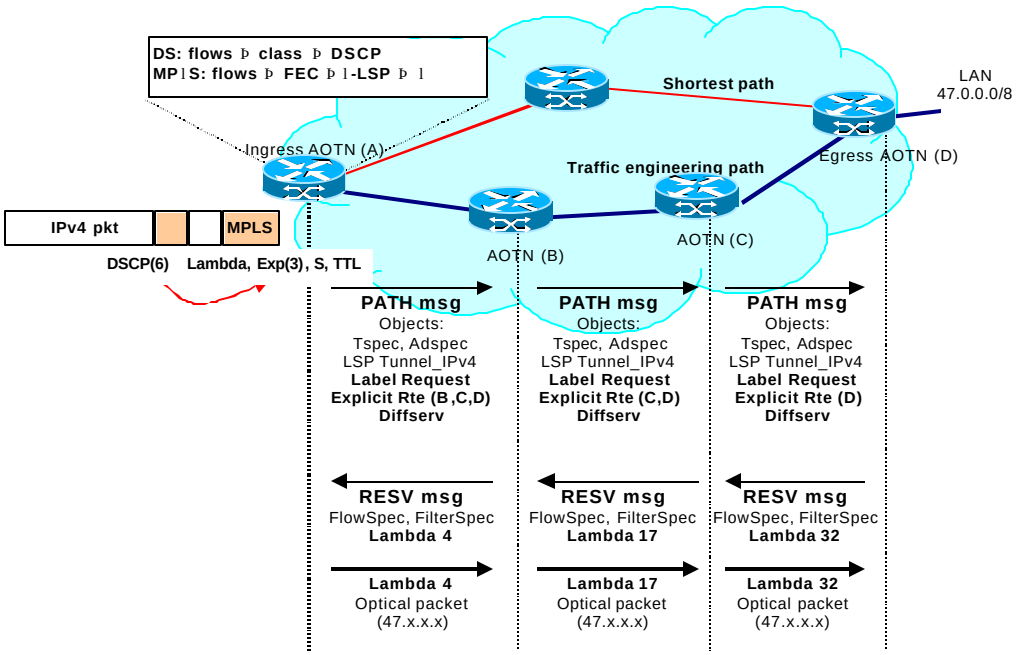

Figure 4. QoS functions at the ingress AOTN node

In the case of DiffServ, the DiffServ-field of the packets is set accordingly since the packets are classified at the edge of the network [9]. In the core of a network, packets are buffered and scheduled in

accordance with their field. On the other hand, with DMS, while packets still have their DiffServ-field set at the edge of the network, the experimental (EXP) field in the MPλS headers is also set according to the Diffserv field. When the packets are flowing upon an optical label switched path (λ-LSP), they are buffered and scheduled in accordance with the EXP field. Whether the MPλS is involved or not in providing QoS, the over-all mechanisms are transparent to the end-users. Sometimes, it is desirable to use different λ-LSPs for different classes of traffic. This causes the physical network to be divided into multiple virtual networks where every virtual network takes care of the corresponding class of traffic. These networks may have different topologies and resources according to their priority. However, these virtual networks can be controlled by constraint-based routing (CBR). The CBR computes constrained-based routes providing explicit-routed λ-Labeled Switched Paths (ER-λ-LSPs) that are subject to the constraints such as bandwidth and administrative policy (see Figure 5). The signaling information such as an explicit route for the constraint-based route can be carried either by Constraint-based Label Distribution Protocol (CR-LDP), or as piggybacked on extensions made to RSVP[10]. Figure 5 shows examples of the λ-LSP establishment process based on DMS concepts using CR-LDP and RSVP extensions.




(a) λ-LSP establishment using CR-LDP




(b) λ-LSP establishment using RSVP extension

Figure 5. λ-LSP establishment process based on DMS concepts

Furthermore, unlike general Diffserv, the DMS could utilize optical layer protection services for the λ-LSP segment that traverses the optical network. That is, the protection services at the MPLS layer for an end-to-end λ-LSP must be mapped onto suitable protection or restoration services offered by the optical layer (Section 4 of this paper treats this). Thus, many λ-LSPs can be aggregated into a single lightpath in AOTN. In [11], 111 and 000 are being used for premium service and best effort service, respectively. As an example of an assured service implementation, Ref. [11] defines the Olympic service, which consists of three service classes: bronze, silver, and gold. So it is possible to assign the different values of EXP field to each class with two more sub classes (low and high drop precedence): Gold: 110, 101; Silver: 100, 011; Bronze: 010, 001.

Figure 6 shows service classification and the example of mapping the MPLS EXP field onto the classification described above, which is defined by the network administrator [12].

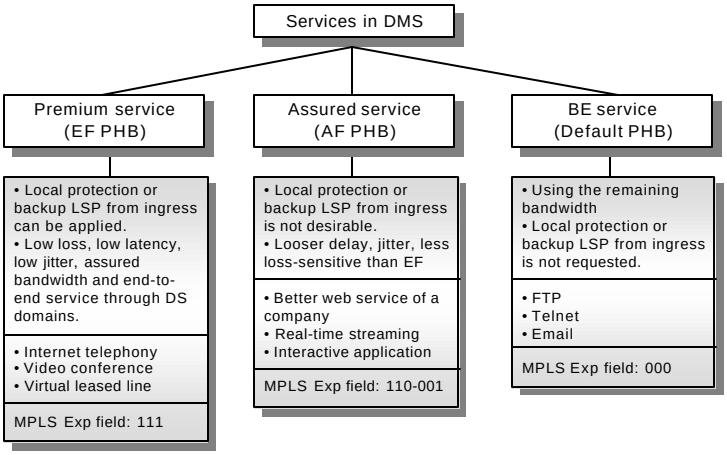



Figure 6. Services in DMS

### 3-3. QoS Management Scheme with QoS Recovery

An architectural model for the AOTN depicted in Figure 2 that defines the DMS domain and captures the concept of end-to-end QoS. In the QoS management functions of the edge AOTN nodes as illustrated in Figure 4, we can identify the functional modules required for providing QoS support in AOTN OXC switches. These include optical packet frame format, resource management functions, and traffic measurements. Optical packet frame format deals with label (lambda) switching, frame delineation and network management information, fast bandwidth provisioning and multiplexing, as well as protection and traffic engineering. Resource management functions consider flow admission control and traffic measurements treat traffic control to meet QoS requirements. These functional and control mechanisms required to provide QoS in AOTN nodes are beyond the scope of this paper. In this paper, we restrict our discussion to the QoS recovery aspect against the degradation of QoS led by device failures or attack-induced faults.

In this regard, within the framework for QoS guarantee based on the DMS model and in order to ensure individual end-to-end QoS guarantees for optical-LSP (λ-LSP), our differentiated QoS protection/restoration schemes are applied to the optical multiplexing section (OMS) level, the optical channel (OCh) level, and the higher-layer at the IP/MPLS layer with the following concepts:

- According to the type of differentiated services (e.g., premium service, assured service, or best-effort service), IP traffic (injected into an ingress AOTN node by conventional domain legacy networks) is segregated (into an optical packet) and associated with a specific optical wavelength (i.e., OCh channel) which consists of many time-division multiplexed channels. Otherwise if there exist several fiber segments, each fiber segment (OMS segment) carries the specific classified set of same-class optical wavelengths.
- Routing and wavelength assignment are accomplished at an ingress AOTN node according to each service class and MPλS. Each optical channel contains a set of IP traffic (or a set of optical packets) of the same service type and a set of optical channels of the same service type

are aggregated on each fiber.

- QoS protection/restoration is accomplished on the same class of service channel or fiber. Section 4 of this paper deals with this issue in detail.
- In absence of fault and intrusion, QoS will be sustained in the core AOTN network. Therefore, each fiber is capable of carrying high-volume IP traffic without QoS degradation.

## 4. QoS Recovery against QoS Degradation caused by Attack-induced Faults

### 4-1. Analysis of Attack Problems

An optical signal undergoes many transmission impairments throughout its route. These impairments range from simple attenuation to complex nonlinear effects and polarization dependent losses. The peculiar behavior of the fiber transmission medium and active/passive elements in the network makes an AOTN vulnerable to unscrupulous attacks, thereby jeopardizing the security of information. These attacks may range from a simple physical access to the medium and its subsequent manipulation, to more complex exploitations of characteristics of optical devices on the link. The attacks related to the physical access of the medium or devices are easier to detect and rectify. On the other hand, attacks exploiting device characteristics necessitate more involved diagnostic expertise, complex remedial measures, and even more systematic detection schemes and control protocols.

There are several factors why optical networks require additional attention in terms of attack modeling. First, optical components and architectures have substantially different accessibility and vulnerabilities from electronic components. For instance, it is fairly straightforward to tap or jam signals at a specific wavelength by bending an optical fiber slightly and either radiating light out of it or coupling light into it [13]. Second, the physical properties of transmission create unique opportunities for the determined attacker. The particular physical property of interest is the transparency of lightpaths. This refers to the fact that, unlike electronic counterparts, optical components along a connection do not process the user payload. Unfortunately, this transparency allows an intruder that has gained access to one component to simply pass a signal right through all the components that handle the associated lightpath. This means that a signal can be forced into the network at a remote location and, by judicious choice of wavelength, affect many different parts of the network. Such a widespread effect is hard to achieve in conventional networks because signals are regenerated at every node, and therefore, a malicious physical signal can be trapped at the ends of a link. Third, optical technology allows for different attack opportunities; for example, the crosstalk level in switches may be sufficiently low for normal operation but may not be low enough to prevent an attacker from transmitting a high-power jamming signal that would disrupt service.

Figure 7 shows a typical AOTN link with ports vulnerable to possible attacks numbered. We present here a brief description of transmission impairments and possible types of attacks each of these ports may experience.

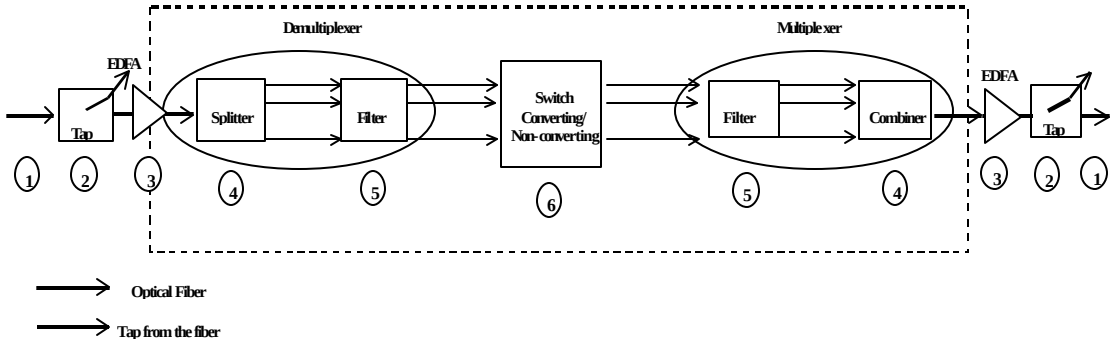



Figure 7. An Optical Cross-Connect (OXC) node.

### 4-1-1. Fiber (attack point 1 in Figure 7)

An optical signal carrying high-speed data will experience attenuation, dispersion, non-linear effects, and polarization dependent losses. While the use of amplifiers can solve attenuation, amplifiers also contribute additional impairments. The use of specific types of fibers (such as dispersion-shifted, polarization-maintaining fibers) may be suggested for reducing dispersion and polarization related degradations, but they, in turn, may introduce other problems such as crosstalk. The unprotected easy access to the physical fiber cable can encourage tampering with by a potential intruder. Simple physical attacks like cutting of the cable can easily be detected by existing metrology techniques and can also be prevented by increasing physical security-related measures. On the other hand, easy physical access to the fiber cable can also cause unauthorized access and subsequent manipulation of the information by way of tapping or by sensing the optical mode leakage. In order to detect this kind of information, more sophisticated measurement techniques are needed.

### 4-1-2. Tap (attack point 2)

The purpose of providing taps is to facilitate easy monitoring, and providing efficient splicing ports for increased demand thereby adding flexibility to the network. Insertion loss and information leakage are associated transmission impairments which can again be eliminated by using amplifiers at the expense of additional vulnerability to attacks as we shall see next. Access to taps also provides an opportunity to the attacker to have access to the signal and to tamper with it by way of either changing the signal power or signal polarization or similar signal properties. This can create problems for subsequent amplifiers and other polarization sensitive network elements and may result in service disruption. Such tampering can be thwarted by minimizing the number of taps and by increasing the physical security in order to prevent access, but detection of a tampered signal may not be easy.

### 4-1-3. Erbium Doped Fiber Amplifiers (attack point 3) [13]

Semiconductor optical amplifiers (SOA) have bandwidths of the order of 100 nm, which is much higher than those of EDFAs (35nm). On the other hand, it is possible to have high gains and output powers with EDFAs. Also, SOAs introduce severe crosstalk when used in WDM systems and so EDFAs are widely preferred and used for an AOTN. In addition to amplified spontaneous emissions (ASE) and

the necessity for flattening the gain spectrum, EDFAs introduce a system penalty in the presence of other interfering channels. This system penalty can be decomposed into two components. The first component arises from the *steady-state* reduction in the amplifier gain due to the increase in the *average* input power. This is also referred to as the *saturation component.* The second component is the component arising from the variation in the gain due to the randomness of the total input power around the mean value. This is known as the *crosstalk component*. It is known that when the number of channels is small, the cross-talk component dominates, but when the number of channels is large, the saturation component dominates. For high data-rate transmission (i.e., data rates much higher than the response time of the amplifier to a change in input power level), the cross-talk component is no longer present and only the steady-state gain reduction is retained. An intruder can easily block transmission of other channels or can disrupt the entire service merely by exploiting this weakness of the EDFAs. Even a legitimate user can cause an attack by transmitting at high power levels so as to deteriorate the EDFA performance. The use of multi-stage EDFAs in a link requires extra precautions and system margins**.** One can detect this kind of attack by *in situ* verification of the following equality around the EDFA if along the link or around the cross-connect or node (if it employs EDFAs as an integral part): $\lambda_i = \lambda_o \pm \lambda_{d/a}$ where $\lambda_i$ is total number of wavelength at the input of the "block" (can be an EDFA or an OXC node), $\lambda_o$ is the total number of wavelengths at its output and $\lambda_{d/a}$ is the total number of wavelengths dropped or added at the node by OADMs. One possible solution we propose to mitigate this type of attack is to equalize gain by way of pre-emphasis and de-emphasis as the case may be, before sending the signals to the EDFA. This can be done by optical processing or by electronic processing with their obvious inherent merits/demerits.

### 4-1-4. Splitter/Combiner (attack point 4)

Typically, a demultiplexer comprises of an optical splitter followed by an optical filter. The power loss introduced by a splitter is its insertion loss. If the splitter itself also performs the function of a filter, it can cause signal degradation and can pose vulnerability to intentional attacks as described below for the case of a filter.

### 4-1-5. Filter (attack point 5)

A good optical filter should have a low insertion loss. The loss should also be independent of the state of polarization of the input signals. The filter should be insensitive to variations in ambient temperature. As more and more filters are cascaded in a WDM system, the passband becomes progressively narrower. To ensure reasonably broad passbands at the end of the cascade, the individual filters should have very flat passbands. At the same time, the passband skirts should be sharp to reduce the amount of energy passed through from the adjacent channels. This energy is seen as crosstalk and degrades the system performance. This crosstalk can also result in an unauthorized access to information. An intentional high power level may subsequently result in high crosstalk levels thereby blocking other legitimate users and can constitute an intrusion. This type of attack is not easy to detect and not easy to rectify on-line. Precautionary measures include power equalization before and after filtering and the use of high quality optical filters.

### 4-1-6. Switch (attack point 6)

An optical switch also is subject to crosstalk due to non-ideal switching. When an interfering signal has been suppressed once with reference to the main signal, it results in a first-order crosstalk. If it is suppressed twice, it results in a second order crosstalk, and so on. Due to multiple switches and multiple nodes in a network, propagation of crosstalk becomes more and more complex. An intruder can also exploit polarization dependent properties of switches and filters to cause service disruption by way of manipulating the signal polarization. A legitimate user can also cause serious threats by changing transmitter power levels and thereby introducing intentional crosstalk to disrupt service or can utilize sensitive reception techniques to gain unauthorized access to the information from crosstalk. While equalizing power levels will eliminate the former type of attack, the latter type of unauthorized information access is not easy to detect. Non-blocking type of switches may also employ wavelength converters and thereby can also contribute to crosstalk in addition to the associated noise, insertion loss and polarization dependent losses.

## 4-2. QoS Protection and Restoration Schemes

### 4-2-1. QoS Recovery for the Optical Channel Level and Higher Layers

One of the advantages that all-optical WDM systems offer is the fact that they are transparent to bit rate, protocol and modulation formats. However, without O/E/O conversions at the cross-connects, guaranteeing uniform QoS for priority specific traffic warrants for monitoring the physical layer devices over the link. Unfortunately, these devices have characteristics that might change linearly or non-linearly depending upon signal parameters like wavelength and its deviations, steady-state and transient power levels, and states of polarization. These parameters can either change under normal network operations like adding/dropping of channels, or can change inherently slowly over time and temperature like states of polarization, nominal wavelength, and amplifier gain or can even change drastically due to an event of any intrusion. Keeping in mind these device level vulnerabilities, the QoS assurance involves a two-level strategy. At higher network layers, since the individual wavelength level monitoring is complex, the administrator should make sure that the high priority signals be assigned wavelengths corresponding to the C-band of the EDFA spectrum. This is especially important in case of cascaded non-gain-clamped EDFAs on the link [14]. If the traffic has a variable priority map, then at least the back-up wavelength should be reserved from the C-band so that high priority traffic signal gets the high QoS recovery path. Additionally, routing a high QoS traffic should employ link power sensitive routing algorithms [15].

Section 4-1 described the general nature of intrusion at various possible attack points of an all-optical cross-connect as shown in Figure 7. Now we see the elements that play part at the physical link level, from the point of view of optical channel level QoS guarantees. For example, EDFAs are the preferred choice for line amplification. Unfortunately, the gain-spectrum of an unclamped EDFA is not flat and shows a peak in the S-band and a fall in the L-band. A cascade of EDFAs even worsens this gain profile. This means that not all the incoming channels will experience uniform gain. Additionally, power levels of incoming channels play a vital role in saturating the EDFA. With only one amplifier in cascade, the increase in power due to channel outages occur rather slowly, in about 100 μs. However with multiple

amplifiers in the chain, the increase in power is much more rapid, with a rise time of a few to tens of μs, and can result in temporary loss of service in the surviving channels. A user can exploit these weaknesses of an EDFA and can cause a QoS threat by way of intrusion unless appropriate precautions (to be described later) are taken.

An optical channel can potentially be indirectly under intrusion induced QoS degradation threat at the demultiplexer. Since the filter stage is not ideal, a cross-talk component will always be present. Higher channel power from a user can create higher cross-talk levels of neighboring users, thereby jeopardizing the QoS guarantee unless power equalization is used before a WDM signal enters the demultiplexer. Due to far-from-ideal characteristics of switching elements employed in a switch module, the demultiplexed channels will have first and higher order cross-talk components along the path. An intruder with unequalized optical channel power can cause QoS threats to other channels. Furthermore, this cross-talk element will also contribute to the non-ideal translation of incoming wavelength if the switch has wavelength converters built-in to reduce blocking. Non-ideal combiners, too, will propagate multiple orders of cross-talk affecting the channel QoS at the multiplexer. This form of indirect intrusion can deteriorate the optical performance of forthcoming EDFAs and other components unless appropriate equalization is used.

Since anomalous functioning of an EDFA can cause more serious threat to the quality of optical channel, the detection algorithm as shown in Figure 8 should be implemented:

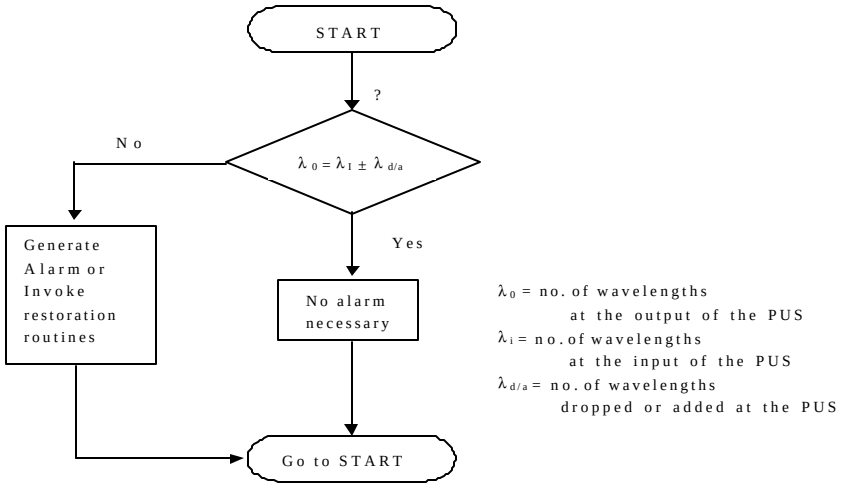



Figure 8. Detection of potential channel service threat at an EDFA.

Premium service provides a guaranteed peak bandwidth service with an end-to-end delay bound. This service has to be accomplished in lightpaths guaranteed to be protected by the optical layer, within a specified recovery time requirement. At channel level, we use local QoS protection mechanisms or the MPLS backup procedure.

Within local protection, upon detecting a failure or attack-induced fault on the primary path, an alternate path is re-established starting from the point of failure within a specified recovery time. This scheme is based on link level hardware protection concepts in a distributed manner. When the degradation

in service is detected because of intrusion on relatively small number of service λ-LSPs, equalizing schemes as described in [15] can be applied locally. In case of a serious threat to the quality of service, the cross-connect must be able to identify the problem and switch to the appropriate protection provision.

To prevent violation of QoS guarantees with the local protection mechanism, the automatic gain control (AGC) system must work very fast (within a few μs) as soon as any intrusion is detected. The simplest scheme for AGC is to monitor the channel power level (as described next) and adjust the pump power to vary the gain accordingly. The response time of this method is ultimately limited by the lifetime of the electrons from the third energy level to the second energy level in Erbium (~1μs). Another scheme of AGC utilizes an optical feedback loop [16] to clamp the amplifier gain. Yet another approach is to introduce an additional wavelength on the link to act as an end-to-end compensating wavelength. The power of this wavelength is varied to complement the power fluctuations in the link. In general, the scheme as illustrated in Figure 9 is required before and/or after an optical component that may be vulnerable to potentially intrusion induced QoS threats.

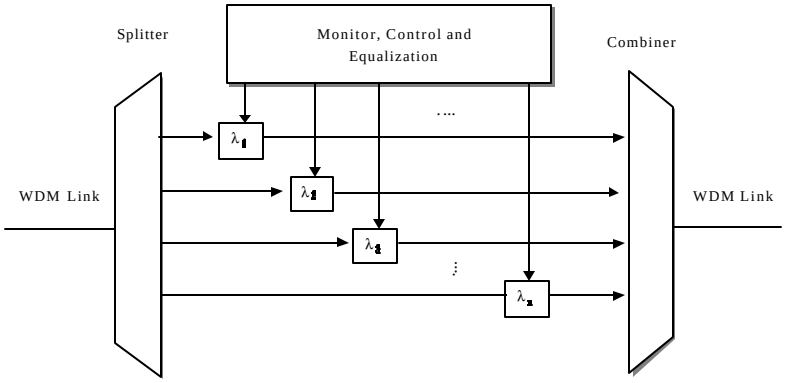



Figure 9. Schematic of an optical power equalizer.

This channel level protection scheme provides less than 50ms protection speed [18].

On the other hand, we can use also the MPL(λ)S backup procedure for sustaining QoS of the premium service. Within this scheme, a premium service is assigned to a specific lightpath (i.e., establishment of λ-LSP), and a backup lightpath is established at the same time. Upon detecting a failure or attack-induced fault on the primary path, a backup path is used to sustain the required QoS. However, the main drawback of this scheme requires signal regeneration at every intermediate node for control mechanisms related to the management of primary and secondary backup paths led by attack or fault isolation and control functions.

The assured service offers an expected level of bandwidth with a statistical delay bound. For sustaining QoS of the assured service, the MPLS LSP restoration scheme is used. The Optical Channel (OCh) path restoration (λ-LSP restoration) scheme requires that every affected working λ-LSP be replaced by a protection ligthpath. This further requires longer restoration completion time since ingress and egress nodes dynamically search for the restoration λ-LSP needed to re-establish the disrupted λ-LSP. Nevertheless restoration can be done in even less time intervals ranging from a few dozen milliseconds to

a few hundred milliseconds.

Best-effort service corresponds to the current Internet service. For sustaining QoS of the best-effort service, we propose a LSP restoration scheme at the IP level. For best-effort traffic, disruptions in service ranging from 100 ms to a few seconds can be compensated by TCP retransmits.

### 4-2-2. QoS Recovery for the Optical Fiber Level

QoS recovery schemes for the optical fiber level (OMS) work at an aggregate signal level, thereby recovering QoS degradation for all lightpaths present on the attacked line or the faulty line containing faulty devices concurrently.

In general, direct access to the physical transmission medium is not so easy. Additionally, there exists a standard mechanism to detect any cut in the fiber - a most obvious type of possible intrusion-led QoS degradation. As shown in Figure 7, designers also provide taps on the path for future extensions and for the purpose of supervisory metrology. In a WDM network, a single fiber can carry a number of wavelengths and hence any service disruption will affect all the priority classes being carried by that fiber under intrusion.

We refer here to a wavelength division multiplexed OTDR technique as demonstrated by Lai, *et al.* [17]. The basic principle behind their proposal is as follows. An OTDR operating at wavelength $\lambda_1$ is combined with a transmitted signal at $\lambda_2$ by a WDM multiplexer as shown in Figure 10.

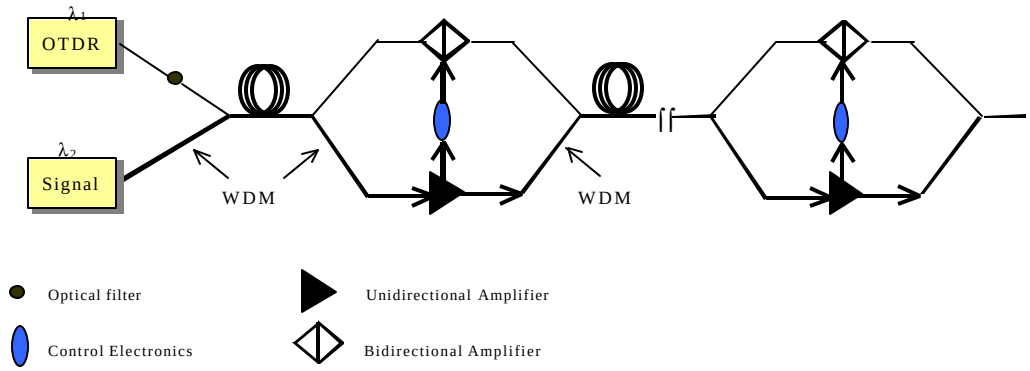



Figure 10. Detection setup for monitoring fiber and EDFA

In order to monitor a fiber cut as well as the unidirectional (because of inserted isolators) EDFAs' status, the OTDR wavelength is passed around each working EDFA by a pair of input/output WDMs. A bi-directional protection optical amplifier can be inserted between the input and output WDMs in order to increase the OTDR dynamic range. The pump laser of bi-directional protection amplifier is used to replace the failed pump laser in a working amplifier under failure condition. If a failure is detected, the entire traffic needs to be switched to the protection fiber. For a SONET ring, this might be simple. But for a WDM mesh network carrying traffic with QoS priority attributes, the issue becomes more complex.

At the level of the multiplex section layer (OMS), different approaches are possible for QoS recovery depending upon the service priority. Premium services command the highest priority and hence 1:1 type of provisioning becomes imperative. The traffic is switched to the dedicated back up as soon as

service degradation is detected. On the other hand, a 1:N type of fixed spare provisioning will be more economical for second priority services with assured guarantee bounds. Upon detecting failure of a device or link, the signal is routed by a 1xN switch to the fixed spare. A 1:N provisionable spare is suited for best-effort priority type of service guarantees. A fixed pool of spare resources is shared via a rotary switch. When a fiber or device is detected to adversely affect the QoS, the signal is switched to the next spare and so on until a free port is found. If no spare is found, QoS restoration may involve upper layers with re-transmit requests.

For each service class, there could be multiple protection options according to the used control algorithms [18], such as dedicated line protection (DLP), optical unidirectional line-switched ring (OULSR), shared line protection (SLP), or shared line-switched WDM self-healing ring (WSHR). In these schemes, protection resources can be either dedicated or shared for OMS protection. OMS protection schemes are also available in mesh network topologies. These mechanisms are being implemented.

Within the proposed differentiated protection/restoration schemes with QoS recovery, the DMS architecture is expected to provide lower cost, more flexible recovery options, and acceptable network utilization for AOTNs.

## 5. Conclusion

An optical signal undergoes many transmission impairments throughout its entire path in an AOTN. Peculiar behavior of transmission medium and active/passive elements on the path makes an AOTN vulnerable to unscrupulous attacks, thereby jeopardizing the security of the information and survivability of the entire network. Unlike TDM-based legacy networks, in case of an AOTN, data travel optically from the source to the destination without any O/E and vice versa conversions. This transparency poses threats against its survivability.

In this paper, we proposed a framework for QoS guarantee based on the DMS model and the QoS recovery schemes to counter QoS degradation led by device failures or attack-induced faults in AOTN. In order to ensure individual end-to-end QoS guarantees for λ-LSP, QoS protection/restoration schemes are envisaged at the OMS level, the OCh level, and the IP/MPLS layer. As one of the client modules, the proposed QoS protection/restoration schemes are being integrated into MERLiN which is a WDM network design and modeling environment in a client/server structure [19]. This environment allows the development and evaluation of distributed algorithms for wavelength assignment and routing, dynamic and traffic driven reconfiguration algorithms, QOS models (parameters, service classes) and protocols for WDM networks, procedures for network management and control, and protocol stacks for transport of IP over WDM (IP/SONET/WDM, IP/MPLS/WDM).

## Acknowledgement

This work was supported in part by the DARPA under grant N66001-00-18949 (co-funded by NSA).

## References


[1] R. Braden, D. Clark, and S. Shenker: Integrated services in the Internet architecture: An overview, Internet RFC 1633, June 1994.

[2] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin: Resource ReSerVation Protocol (RSVP)-Version 1, Functional specification, Internet RFC 2205, IETF, September 1997.

[3] S. Shenker, C. Partridge, and R. Guerin: Specification of the guaranteed quality of service, Internet RFC 2212, September 1997.

[4] V. Jacobson, K. Nichols, and K. Poduri: An expedited forwarding PHB, Internet RFC 2598, June 1999.

[5] Su-Kyoung Lee and Sung-Un Kim: Standards activities for optical transport networks in ITU-T, Optical Network Magazine, vol. 2, no. 2, (March-April 2001), pp. 82-84.

[6] D. Awduche, Y. Rekhter, J. Drake, and R. Coltun: Multi-Protocol lambda switching: Combining MPLS traffic engineering control with optical crossconnects," IETF Internet Draft, draft-awduche-mpls-te-optical-03.txt, April 2001, work in progress.

[7] J. Patel, S. Kim, D. Su: Attack management for all optical transport networks, submitted to IEEE Journal on Survey and Tutorial.

[8] A. Jukan, A. Monitzer, and H.R. van As: QoS-restorability in optical networks, Proc. of 24th European Conference on Optical Communication (ECOC'98), vol. 1, (Madrid, Spain, September 20-24, 1998), pp. 711-712.

[9] K. Nicholas, S. Blake, F. Baker and D. Black: Definition of the differentiated services field (DS Field) in IPv4 and IPv6 headers, Internet RFC 2474, IETF, December 1998.

[10] B. Jamousi: Constraint-based LSP setup using LDP, Internet draft-ietf-mpls-crldp-04.txt, IETF, July 2000.

[11] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski: Assured forwarding PHB group, Internet RFC 2597, June 1999.

[12] N. Golmie, T.D. Ndousse, and D. Su: Differented optical services model for WDM networks, IEEE Communications Magazine, vol. 38, no. 2, (February 2000), pp. 68-73.

[13] R. Ramaswami and K. N. Sivarajan: Optical networks: A practical perspective, Morgan Kaufmann Publishers, Inc., San Francisco, CA, 1998.

[14] S. R. Chin: Simplified modeling of transients in gain-clamped erbium-doped fiber amplifier, IEEE/OSA Journal of Lightwave Technology, vol. 16, no. 6, (June 1998), pp. 1095-1100.

[15] M. Ali, B. Ramamurthy, and J. S. Deogun: Routing and wavelength assignment (RWA) with power considerations in all-optical wavelength-routed networks, Proc. of 1999 IEEE Global Communications Conference (GLOBECOM'99), vol. 2, (Rio de Janeiro, Brazil, December 5-9, 1999), pp. 1433-1437.

[16] L. Gillner, C. P. Larsen, and M. Gustavsson: Scalability of optical multiwavelength networks: crosstalk analysis, IEEE/OSA Journal of Lightwave Technology, vol. 17, no. 1, (January 1999), pp. 58- 67.

[17] Y. W. Lai, Y. K. Chen, and W. I. Way: Novel supervisory technique using wavelength-division-multiplexed OTDR in EDFA repeatered transmission systems, IEEE Photonics Technology Letters, vol. 6, no. 3, (March 1994), pp. 446-449.

[18] A. Fumagalli, and L. Valcarengh: IP restoration vs. WDM protection: Is there an optimal choice?" IEEE Network, vol. 14, no. 6, (November/December 2000), pp. 34-41.

[19] http://w3.antd.nist.gov/Hsntg/prd_merlin.html.

**Jigesh K. Patel**
**High Speed Network Technologies Group**
**National Institute of Standards and Technology**
**Gaithersburg, MD 20899, USA**
**patel@antd.nist.gov**

Jigesh K. Patel received his B. Eng. from Sardar Patel University, India in 1988, M. Eng. from University of Roorkee, India in 1995. Since 1999, he has been with Advanced Network Technologies Division at the National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA as a Guest Researcher. He has published extensively in refereed journals and conference proceedings. His research areas include DWDM networks and wireless optical communications. He is a member of Sigma Xi, a senior member of IEEE and a member of SPIE.

**Sung U. Kim**
**High Speed Network Technologies Group**
**National Institute of Standards and Technology**
**Gaithersburg, MD 20899, USA**
**kimsu@antd.nist.gov**

Sung U. Kim received B.S. from Kyoungpuk National University, Korea in 1982 and received M.S. and Ph.D. degree in Computer Science from the University of Paris 7, France in 1990 and 1993, respectively. He joined Electronics and Telecommunications Research Institute (ETRI, Korea) in 1982 and then Korea Telecom Research Labs (KTRL) in 1985, where he had developed protocol testing systems for LAN, B-ISDN and Intelligent Network and developed also a protocol validation tool. He was also an editor for ITU-T SG7 Q.23 on data communication protocol testing. Since 1995, he has been an assistant professor in the Department of Telematics Engineering, Pukyong National University, Korea. Currently he is a Guest Researcher with Advanced Network Technologies Division at NIST of USA. His research interests include protocol engineering, MPLS, DWDM optical network and QoS.

**David H. Su**
**High Speed Network Technologies Group**
**National Institute of Standards and Technology**
**Gaithersburg, MD 20899, USA**
**dsu@nist.gov**

David H. Su is the manager of the High-Speed Network Technologies Group of the Information Technology Laboratory at NIST. His main research interests are in modeling, testing, and performance measurement of communications protocols. He has been involved in modeling and evaluation of protocols as they were being developed by standardization organizations. These include protocols for ATM networks, hybrid fiber coaxial networks, optical networks, and picocell wireless networks. He has also participated in the development of standard conformance test suites for testing of X.25, ISDN, FDDI, and ATM network protocols. Before joining NIST in 1988, he was with GE Information Service Company as the manager of internetworking software for support of GE's worldwide data network. From 1973 to 1976 he was an assistant professor in computer science at Florida International University, Miami. He received his Ph.D. degree in computer science from the Ohio State University in 1974.